PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-027911
(43)Date of publication of application : 30.01.2001

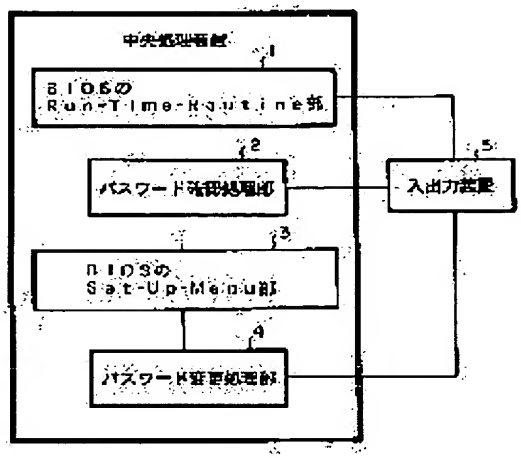
(51)Int.Cl. G06F 1/00
G06F 15/00

(21)Application number : 11-200635
(22)Date of filing : 14.07.1999

(71)Applicant : NEC SOFTWARE KYUSHU LTD
(72)Inventor : HASHIMOTO KAZUAKI

(54) SYSTEM AND METHOD FOR PREVENTING ILLEGAL ACCESS OF COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal access to the inner part of a personal computer in the power supply stage of the personal computer.
SOLUTION: A Run-Time-Routine part 1 has a means which is started by as instruction after a user turns on the power of a personal computer, displays a password input screen on an input/output device 5 before an operating system(OS) is started through a password recognition processing part 2, urges the input of a password, compares the inputted password with a password which is previously set by a password change processing part 4, displays a warning message on the input/output device 5 when the password is illegal, urges the input of the password again when the number of display times on the warning message is up to two times, turns off the power of the computer when the number of display times is three times and starts OS when the inputted password is correct.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－27911
（P2001－27911A）
(43)公開日　平成13年１月30日(2001.1.30)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ 1/00	３７０Ｅ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ｂ	

審査請求　有　　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平11－200635

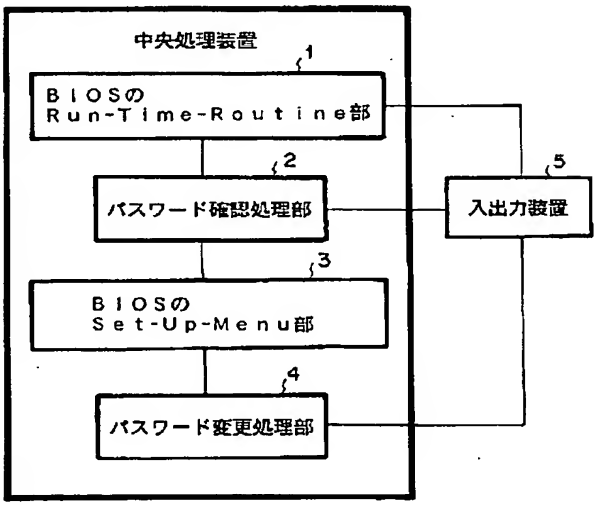
(22)出願日　平成11年７月14日(1999.7.14)

(71)出願人　000164449
九州日本電気ソフトウェア株式会社
福岡市早良区百道浜２丁目４－１　ＮＥＣ九州システムセンター
(72)発明者　橋本　和明
福岡県福岡市早良区百道浜２－４－１　九州日本電気ソフトウェア株式会社内
(74)代理人　100065385
弁理士　山下　穣平

Ｆターム(参考)　5B085 AC02 AE03

(54)【発明の名称】　コンピュータの不正アクセス防止システムとその方法

(57)【要約】
【課題】　パーソナルコンピュータの電源投入段階で、パーソナルコンピュータ内部への不正なアクセスを防止する。
【解決手段】　Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１は、使用者が、パソコンの電源をＯＮにした後の指示により起動し、パスワード確認処理部２を介して、オペレーティングシステム（ＯＳ）を起動する前にパスワード入力画面を入出力装置５上に表示してパスワード入力を促し、入力されたパスワードを、パスワード変更処理部４で予め設定されたパスワードと比較し、パスワードが不正な場合に、入出力装置５上に警告メッセージを表示し、警告メッセージの表示回数が２回までならば再度、パスワード入力を促し、表示回数が３回目である場合にはコンピュータの電源をＯＦＦにし、さもなくて、入力されたパスワードが正しい場合には、ＯＳの起動を行う手段を有する。



1

【特許請求の範囲】

【請求項１】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止システムであって、

前記オペレーティングシステムは、ＢＩＯＳ（Basic I/O System）のＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部と、ＢＩＯＳのＳｅｔ－Ｕｐ－Ｍｅｎｕ部と、パスワード確認処理部と、パスワード変更処理部とを備え、

前記パスワード変更処理部は、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定する手段を備え、

前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部は、使用者が、パソコンの電源をＯＮにした後の指示により起動し、パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促す手段と、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較する手段と、前記パスワードが不正な場合に、前記入出力装置上に警告メッセージを表示し、前記警告メッセージの表示回数が所定回数より少ないならば再度、前記パスワード入力を促す手段を実行し、前記警告メッセージの表示回数が前記所定回数以上である場合には前記コンピュータの電源をＯＦＦにする手段と、さもなくて、前記入力されたパスワードが正しい場合には、前記オペレーティングシステムの起動を行う手段と、

を有することを特徴とするコンピュータの不正アクセス防止システム。

【請求項２】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止システムであって、

前記オペレーティングシステムは、ＢＩＯＳ（Basic I/O System）のＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部と、ＢＩＯＳのＳｅｔ－Ｕｐ－Ｍｅｎｕ部と、パスワード確認処理部と、パスワード変更処理部とを備え、

前記パスワード変更処理部は、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定する手段を備え、

前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部は、使用者が、パソコンの電源をＯＮにした後の指示により起動し、パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促す手段と、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較する手段と、前記パスワードが不正な場合に、前記コンピュータの電源をＯＦＦにする手段と、さもなくて、前記パスワードの照合が取れた場合に、使用者に前記パスワード変更処理部を前記入出力装置からの指示により呼び出させる手段を備え、

前記呼び出されたパスワード変更処理部は、前記入出力装置上に、パスワードを更新するか否かを旨とするメッセージを表示する手段と、該表示後に、使用者に、前記入出力装置から、パスワードを更新するか否かを選択入力せしめる手段と、該選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていた場合には、前記入出力装置から引き続き入力されたパスワードを管理領域に書き込み、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部にオペレーティングシステムを起動するように設定して、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部によるオペレーティングシステムの起動を行わせる手段と、さもなくて、前記選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていなかった場合には、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部が、オペレーティングシステムの起動を行う手段と、

を有することを特徴とするコンピュータの不正アクセス防止システム。

【請求項３】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータのための不正アクセス防止方法であって、

前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定するステップと、

パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促すステップと、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較するステップと、前記パスワードが不正な場合に、前記入出力装置上に警告メッセージを表示し、前記警告メッセージの表示回数が所定回数より少ないならば再度、前記パスワード入力を促すステップを実行し、前記警告メッセージの表示回数が前記所定回数以上である場合には前記コンピュータの電源をＯＦＦにするステップと、さもなくて、前記入力されたパスワードが正しい場合には、前記オペレーティングシステムの起動を行うステップと、

を有することを特徴とするコンピュータの不正アクセス防止方法。

【請求項４】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止方法であって、

前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワ

ードを予め設定するステップと、
パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促すステップと、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較するステップと、前記パスワードが不正な場合に、前記コンピュータの電源をＯＦＦにするステップと、さもなくて、前記パスワードの照合が取れた場合に、使用者に前記パスワード変更処理部を前記入出力装置からの指示により呼び出させるステップと、
前記入出力装置上に、パスワードを更新するか否かを旨とするメッセージを表示するステップと、該表示後に、使用者に、前記入出力装置から、パスワードを更新するか否かを選択入力せしめるステップと、該選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていた場合には、前記入出力装置から引き続き入力されたパスワードを管理領域に書き込み、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部にオペレーティングシステムを起動するように設定して、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部によるオペレーティングシステムの起動を行わせるステップと、さもなくて、前記選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていなかった場合には、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部が、オペレーティングシステムの起動を行うステップと、
を有することを特徴とするコンピュータの不正アクセス防止方法。

【請求項５】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記不正アクセス防止方法は、
前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定するステップと、
パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促すステップと、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較するステップと、前記パスワードが不正な場合に、前記入出力装置上に警告メッセージを表示し、前記警告メッセージの表示回数が所定回数より少ないならば再度、前記パスワード入力を促すステップを実行し、前記警告メッセージの表示回数が前記所定回数以上である場合には前記コンピュータの電源をＯＦＦにするステップと、さもなくて、前記入力されたパスワードが正しい場合には、前記オペレーティングシステムの起動を行うステップと、
を有することを特徴とするコンピュータ読み込み可能な記録媒体。

【請求項６】　ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記不正アクセス防止方法は、
前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定するステップと、
パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促すステップと、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較するステップと、前記パスワードが不正な場合に、前記コンピュータの電源をＯＦＦにするステップと、さもなくて、前記パスワードの照合が取れた場合に、使用者に前記パスワード変更処理部を前記入出力装置からの指示により呼び出させるステップと、
前記入出力装置上に、パスワードを更新するか否かを旨とするメッセージを表示するステップと、該表示後に、使用者に、前記入出力装置から、パスワードを更新するか否かを選択入力せしめるステップと、該選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていた場合には、前記入出力装置から引き続き入力されたパスワードを管理領域に書き込み、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部にオペレーティングシステムを起動するように設定して、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部によるオペレーティングシステムの起動を行わせるステップと、さもなくて、前記選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていなかった場合には、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部が、オペレーティングシステムの起動を行うステップと、
を有することを特徴とするコンピュータの不正アクセス防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータの不正アクセス防止システムに関し、特に、ＢＩＯＳ（Basic I/O System）を搭載したパーソナルコンピュータの不正アクセス防止システムとその方法に関する。

【０００２】

【従来の技術】従来、Microsoft社のＯＳ（Ｗｉｎｄｏ

ｗｓ９５，９８）を搭載したコンピュータにおけるセキュリテイ対策には、Microsoftネットワークへのログイン時に実施されるものとして、Microsoft Windowsログオン等の対策がある。

【０００３】本発明の分野に関連する従来技術を過去の特許出願から遡及調査すると、まず、特開昭６０－２２３２４６号公報には、センタ装置に接続された端末装置の不正使用を防ぐ目的で、センタ装置側に端末装置に対応する端末番号とパスワードとを記録しておき、端末装置側から送られてきたパスワードを、センタ装置側で、端末番号を確認して照合する技術が開示されている。

【０００４】なお、電源投入後のＢＩＯＳ（Basic I/O System）の起動によるパスワードの検証によっても電源がＯＦＦにされない方式に関する出願としては、特開平６－１０３２３５号公報，特開平８－１４７０６２号公報，特開平１０－１８７６１８号公報に開示する技術がある。

【０００５】

【発明が解決しようとする課題】しかし、従来の技術では、不正な使用者が、フロッピィディスクによりパソコン（パーソナルコンピュータ）を起動した場合、パソコン上のアプリケーションソフトウェアは起動できないが、ファイルのコピーと削除は依然として可能であるため、上記セキュリティ対策では十分な対策が取られているとは言えない。

【０００６】また、これまではシステム全体でセキュリティを考えていたが、近来のパソコンの性能の飛躍的な向上により、今後は、個々のパソコン単位でのセキュリティ対策が重要課題として浮上してくるものと考えられる。

【０００７】本発明は、以上のような従来のコンピュータの不正アクセス防止システムにおける問題点に鑑みてなされたものであり、パーソナルコンピュータの電源投入段階で、パーソナルコンピュータ内部への不正なアクセスを防止することができるコンピュータの不正アクセス防止システムとその方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明によるコンピュータの不正アクセス防止システムは、ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止システムであって、前記オペレーティングシステムは、ＢＩＯＳ（Basic I/O System）のＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部と、ＢＩＯＳのＳｅｔ－Ｕｐ－Ｍｅｎｕ部と、パスワード確認処理部と、パスワード変更処理部とを備え、前記パスワード変更処理部は、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定する手段を備え、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部は、使用者が、パソコンの電源をＯＮにした後の指示により起動し、パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促す手段と、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較する手段と、前記パスワードが不正な場合に、前記入出力装置上に警告メッセージを表示し、前記警告メッセージの表示回数が所定回数より少ないならば再度、前記パスワード入力を促す手段を実行し、前記警告メッセージの表示回数が前記所定回数以上である場合には前記コンピュータの電源をＯＦＦにする手段と、さもなくて、前記入力されたパスワードが正しい場合には、前記オペレーティングシステムの起動を行う手段と、を有することを特徴とする。

【０００９】また、本発明によるコンピュータの不正アクセス防止システムは、ディスプレイ装置とキーボードを含む入出力装置を備え、オペレーティングシステムの制御下で動作するコンピュータの不正アクセス防止システムであって、前記オペレーティングシステムは、ＢＩＯＳ（Basic I/O System）のＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部と、ＢＩＯＳのＳｅｔ－Ｕｐ－Ｍｅｎｕ部と、パスワード確認処理部と、パスワード変更処理部とを備え、前記パスワード変更処理部は、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部により制御されてパスワードを予め設定する手段を備え、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部は、使用者が、パソコンの電源をＯＮにした後の指示により起動し、パスワード確認処理部を介して、前記オペレーティングシステムを起動する前にパスワード入力画面を前記入出力装置上に表示して使用者にパスワード入力を促す手段と、前記パスワード入力画面の表示により、使用者が前記入出力装置からパスワードを入力した時に、該入力されたパスワードを、前記パスワード変更処理部で予め設定されたパスワードと比較する手段と、前記パスワードが不正な場合に、前記コンピュータの電源をＯＦＦにする手段と、さもなくて、前記パスワードの照合が取れた場合に、使用者に前記パスワード変更処理部を前記入出力装置からの指示により呼び出させる手段を備え、前記呼び出されたパスワード変更処理部は、前記入出力装置上に、パスワードを更新するか否かを旨とするメッセージを表示する手段と、該表示後に、使用者に、前記入出力装置から、パスワードを更新するか否かを選択入力せしめる手段と、該選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていた場合には、前記入出力装置から引き続き入力されたパスワードを管理領域に書き込み、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部にオペレーティングシステムを起動するように設定して、前記Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部によるオペレーティングシステムの起動を行わせる手

段と、さもなくて、前記選択入力の内容を検証した結果、パスワードを更新する旨の入力がなされていなかった場合には、前記Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部が、オペレーティングシステムの起動を行う手段と、を有することを特徴とする。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００１１】（第１の実施の形態）図１は、本発明の第１の実施の形態に係るコンピュータの不正アクセス防止システムの全体構成を示すブロック図である。

【００１２】本実施の形態に係るコンピュータの不正アクセス防止システムは、ＢＩＯＳのＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１と、パスワード確認処理部２と、ＢＩＯＳのＳｅｔ－Ｕｐ－Ｍｅｎｕ部３と、パスワード変更処理部４と、ディスプレイ装置、キーボードからなる入出力装置５とを含む。

【００１３】パスワード確認処理部２は、使用者によって、パソコン（パーソナルコンピュータ）の電源がＯＮにされると、Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１からの要求を受けて、使用者にパスワードの入力を行わせる。パスワード確認処理部２は、引き続き、入出力装置５のキーボードで入力されたパスワードを、Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部３管轄下のパスワード変更処理部４で登録されたパスワードと比較し、正しいパスワードであればオペレーティングシステムの起動を行う。上記入力されたパスワードが不正であれば、３回再入力を促し、それでも不正なパスワードが入力された場合、不正なパスワードである旨のメッセージを入出力装置５のディスプレイ装置に表示した後、電源をＯＦＦにする。

【００１４】図２は、本発明の第１の実施の形態に係るコンピュータの不正アクセス防止システムの動作を示すフローチャートである。

【００１５】以下、図１を参照しつつ、図２に示すフローチャートを使用して、本実施の形態に係るセキュリティシステムの動作を説明する。

【００１６】まず、ステップＡでは、使用者が、パソコンの電源をＯＮにした後で、Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１を起動する旨の指示を行う。

【００１７】上記使用者からの指示により、Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１が起動する。

【００１８】ステップＢでは、上記起動したＲｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１からの指示により、パスワード確認処理部２が、オペレーティングシステムを起動する前に、パスワード入力画面を入出力装置５のディスプレイ装置に表示せしめ、使用者にパスワードの入力を促す。ここで、使用者は、パスワードを入出力装置５のキーボードから入力する。

【００１９】上記入力要求により、使用者が入出力装置５のキーボードからパスワードを入力したならば、ステップＣにて、パスワード確認処理部２は、上記入力されたパスワードを、パスワード変更処理部４で予め設定されたパスワードと比較し、上記パスワードが不正な場合は、ステップＤにて、パスワード確認処理部２が入出力装置５のディスプレイ装置上に警告メッセージを表示した後、警告メッセージの表示回数のカウンタをカウントアップし、ステップＦにて、警告メッセージの表示回数が２回までならステップＢに戻して、再度、パスワードの入力を促す。さもなくて、上記入力されたパスワードが入出力装置５のキーボードから入力された３回目の不正なパスワードである場合、パスワード確認処理部２はパソコンの電源をＯＦＦにする。

【００２０】ステップＣにおいて、上記入力されたパスワードが正しい場合は、オペレーティングシステムの起動を行う。

【００２１】（第２の実施の形態）本実施例に係るコンピュータの不正アクセス防止システムの全体構成は、本発明の第１の実施の形態に係るコンピュータの不正アクセス防止システムの全体構成と同じである。しかし、その構成要素間の連携動作は、第１の実施の形態とは異なる。

【００２２】図３は、本発明の第２の実施の形態に係るコンピュータの不正アクセス防止システムの動作を示すフローチャートである。

【００２３】以下、図１を参照しつつ、図３に示すフローチャートを使用して、本実施の形態に係るセキュリティシステムの動作を説明する。

【００２４】まず、ステップＡでは、使用者が、パソコンの電源ＯＮにした後で、Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部３を起動する旨の指示を行う。

【００２５】ステップＢ１では、上記起動したＳｅｔ－Ｕｐ－Ｍｅｎｕ部３からの指示により、パスワード確認処理部２が、オペレーティングシステムを起動する前に、パスワード入力画面を入出力装置５のディスプレイ装置に表示せしめ、使用者にパスワードの入力を促す。ここで、使用者は、パスワードを入出力装置５のキーボードから入力する。

【００２６】ステップＣ１では、パスワード確認処理部２が、上記入力されたパスワードをパスワード変更処理部４で予め設定されているパスワードと照合する。

【００２７】上記パスワードの照合が取れない場合（使用者によるパスワード入力が失敗した場合）、ステップＤ１にて、パスワード確認処理部２は、パソコンの電源をＯＦＦにする。

【００２８】上記パスワードの照合が取れた場合（使用者によるパスワード入力が成功した場合）、ステップＥ１では、使用者が、入出力装置５のキーボードにてパスワード変更処理部４を呼び出し、実行せしめる。

【００２９】これにより、入出力装置５のディスプレイ装置上に、“パスワードを更新するか否か”を旨とする

メッセージが表示されるので、使用者は、入出力装置５のキーボードから、パスワードを更新するか否かを選択入力する。使用者は、パスワードを更新する場合には、入出力装置５のキーボードから「Ｙｅｓ」を入力し、パスワードを更新しない場合には、入出力装置５のキーボードから「Ｎｏ」を入力する。

【００３０】ステップＦ１では、上記の選択入力の内容を検証し、パスワードを更新する旨の入力がなされていた場合には、そのまま下記のステップＧ１に移る。（パスワードを更新する旨の入力がなされていなかった場合には、制御の流れを後述するステップＨ１に移す。）ステップＧ１では、使用者は、パスワードを入出力装置５のキーボードから入力する。上記入力されたパスワードは、パスワード変更処理部２が管理しているエリアに書き込まれる。

【００３１】ステップＨ２では、パスワード確認処理部２が、Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１にオペレーティングシステムを起動するように設定して、Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部１によるオペレーティングシステムの起動を行う。

【００３２】ステップＨ１では、Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部３が、オペレーティングシステムの起動を行う。

【００３３】なお、図２，図３のフローチャートで示したプログラムなど、処理装置に上記の処理を行わせるためのプログラムは、ＣＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に格納して配付してもよい。そして、少なくともマイクロコンピュータ，パーソナルコンピュータ，汎用コンピュータを範疇に含むコンピュータが、上記の記録媒体から上記プログラムを読み出して、実行するものとしてもよい。

【００３４】

【発明の効果】以上説明した本発明によれば、従来のオペレーティングシステムでは防止できなかったコンピュータへの不正なアクセスを、パーソナルコンピュータの電源投入段階で防止することが可能となり、豊富なアプリケーションを備えたオペレーティングシステムを、不正使用者によるファイルのコピーや削除の心配を無くして、安心して使用することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係るコンピュータの不正アクセス防止システムの全体構成を示すブロック図である。

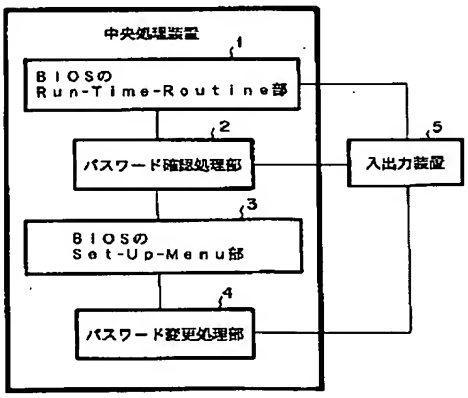
【図２】本発明の第１の実施の形態に係るコンピュータの不正アクセス防止システムの動作を示すフローチャートである。

【図３】本発明の第２の実施の形態に係るコンピュータの不正アクセス防止システムの動作を示すフローチャートである。

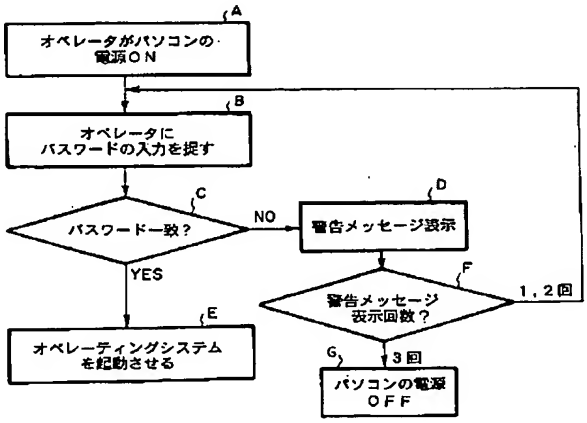
【符号の説明】

１　Ｒｕｎ－Ｔｉｍｅ－Ｒｏｕｔｉｎｅ部
２　パスワード確認処理部
３　Ｓｅｔ－Ｕｐ－Ｍｅｎｕ部
４　パスワード変更処理部
５　入出力装置

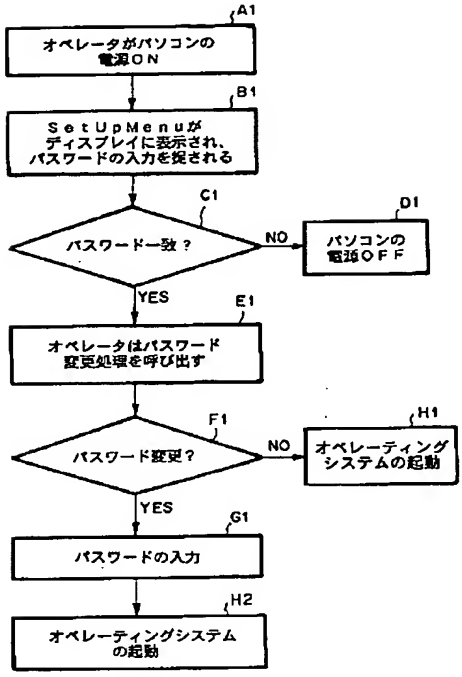
【図１】



【図２】



【図３】


A1
オペレータがパソコンの電源ON
B1
SetUpMenuがディスプレイに表示され、パスワードの入力を促される
C1
パスワード一致？
NO
D1
パソコンの電源OFF
YES
E1
オペレータはパスワード変更処理を呼び出す
F1
パスワード変更？
NO
H1
オペレーティングシステムの起動
YES
G1
パスワードの入力
H2
オペレーティングシステムの起動

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]An illegal access prevention system of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system characterized by comprising the following.
Said operating system is a Run-Time-Routine part of BIOS (Basic I/O System).
A Set-Up-Menu part of BIOS.
A password confirmation treating part.
Have a password change treating part and said password change treating part, Have a means for it to be controlled by said Set-Up-Menu part, and to set up a password beforehand, and said Run-Time-Routine part, A user starts with the directions after turning ON a power supply of a personal computer, and via a password confirmation treating part, By means to display a password input screen on said input/output device, and to demand password input from a user before starting said operating system, and the display of said password input screen. A means in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device, When said password is inaccurate, a warning message is displayed on said input/output device, A means which will perform again a means urged to said password input if there is less display frequency of said warning message than prescribed frequency, and turns OFF a power supply of said computer when display frequency of said warning message is more than said prescribed frequency, A means by which there is nothing as if and said entered password starts said operating system to a right case.

[Claim 2]An illegal access prevention system of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system characterized by comprising the following.
Said operating system is a Run-Time-Routine part of BIOS (Basic I/O System).
A Set-Up-Menu part of BIOS.
A password confirmation treating part.
Have a password change treating part and said password change treating part, Have a means for it to be controlled by said Set-Up-Menu part, and to set up a password beforehand, and said Set-Up-Menu part, A user starts with the directions after turning ON a power supply of a personal computer, and via a password confirmation treating part, By means to display a password input screen on said input/output device, and to demand password input from a user before starting said operating system, and the display of said password input screen. A means in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device, A means which turns OFF a power supply of said computer when said password is inaccurate, When there is nothing as if and collation of said password is able to be taken, it has a means to which a user is made to call said password change treating part with the directions from said input/output device, A means by which said called password change treating part displays a message which makes it a purport whether to update a password or not on said input/output device, and a means, to which a user does the selection input of whether a password is updated or not from said input/output device after this display, As a result of verifying the contents of this selection input, when an input of a purport that a password is updated is made, Write a password succeedingly entered from said input/output device in a management domain, and it sets up start an operating system in said Run-Time-Routine part, A means to start an operating system by said Run-Time-Routine part, A means by which said Set-Up-Menu part starts an operating system when an input of a purport that a password is updated is not made, as a result of there being nothing as if and verifying the contents of said selection input.

[Claim 3]An unauthorized access prevention method characterized by comprising the following for a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system.
A step which is controlled by said Set-Up-Menu part, and sets up a password beforehand.
A step which displays a password input screen on said input/output device, and demands password input from a user via a password confirmation treating part before starting said operating system.
A step in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device by the display of said password input screen.
When said password is inaccurate, a warning message is displayed on said input/output device, If there is less display frequency of said warning message than prescribed frequency, a step urged to said password input will be performed again, A step which turns OFF a power supply of said computer when display frequency of said warning message is more than said prescribed frequency, and a step to which there is nothing as if and said entered password starts said operating system to a right case.

[Claim 4]An unauthorized access prevention method of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system characterized by comprising the following.
A step which is controlled by said Set-Up-Menu part, and sets up a password beforehand.
A step which displays a password input screen on said input/output device, and demands password input from a user via a password confirmation treating part before starting said operating system.
A step in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device by the display of said password input screen.
A step which turns OFF a power supply of said computer when said password is inaccurate, A step to which a user is made to call said password change treating part with the directions from said input/output device when there is nothing as if and collation of said password is able to be taken, A step which displays a message which makes it a purport whether to update a password or not on said input/output device, A step to which a user does the selection input of whether a password is updated or not from said input/output device after this display, As a result of verifying the contents of this selection input, when an input of a purport that a password is updated is made, Write a password succeedingly entered from said input/output device in a management domain, and it sets up start an operating system in said Run-Time-Routine part, A step which starts an operating system by said Run-Time-Routine part, A step to which said Set-Up-Menu part starts an operating system when an input of a purport that a password is updated is not made, as a result of there being nothing as if and verifying the contents of said selection input.

[Claim 5]A recording medium characterized by comprising the following which recorded a program for making a computer perform an unauthorized access prevention method of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system and in which computer reading is possible.
A step which said unauthorized access prevention method is controlled by said Set-Up-Menu part, and sets up a password beforehand.
A step which displays a password input screen on said input/output device, and demands password input from a user via a password confirmation treating part before starting said operating system.
A step in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device by the display of said password input screen.
When said password is inaccurate, a warning message is displayed on said input/output device, If there is less display frequency of said warning message than prescribed frequency, a step urged to said password input will be performed again, A step which turns OFF a power supply of said computer when display frequency of said warning message is more than said prescribed frequency, and a step to which there is nothing as if and said entered password starts said operating system to a right case.

[Claim 6]A recording medium characterized by comprising the following which recorded a program for making a computer perform an unauthorized access prevention method of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system and

in which computer reading is possible.
A step which said unauthorized access prevention method is controlled by said Set-Up-Menu part, and sets up a password beforehand.
A step which displays a password input screen on said input/output device, and demands password input from a user via a password confirmation treating part before starting said operating system.
A step in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device by the display of said password input screen.
A step which turns OFF a power supply of said computer when said password is inaccurate, A step to which a user is made to call said password change treating part with the directions from said input/output device when there is nothing as if and collation of said password is able to be taken, A step which displays a message which makes it a purport whether to update a password or not on said input/output device, A step to which a user does the selection input of whether a password is updated or not from said input/output device after this display, As a result of verifying the contents of this selection input, when an input of a purport that a password is updated is made, Write a password succeedingly entered from said input/output device in a management domain, and it sets up start an operating system in said Run-Time-Routine part, A step which starts an operating system by said Run-Time-Routine part, A step to which said Set-Up-Menu part starts an operating system when an input of a purport that a password is updated is not made, as a result of there being nothing as if and verifying the contents of said selection input.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the illegal access prevention system and method of the personal computer which carries BIOS (Basic I/O System) about the illegal access prevention system of a computer.
[0002]
[Description of the Prior Art]Conventionally, there are measures, such as Microsoft Windows logon, in the security countermeasures in the computer which carries OS (Windows 95, 98) of Microsoft Corp. as what is carried out at the time of login to the Microsoft network.
[0003]When retroactivity investigation of the conventional technology relevant to the field of this invention is conducted from the past patent application, first to JP,60-223246,A. For the purpose of preventing the unauthorized use of the terminal unit connected to the center apparatus, the terminal number and password corresponding to a terminal unit are recorded on the center apparatus side, and the art which checks a terminal number and compares the password sent from the terminal unit side by the center apparatus side is indicated.
[0004]A power supply as application about the method which is not turned OFF also by verification of the password by starting of BIOS (Basic I/O System) after powering on, There is art indicated to JP,6-103235,A, JP,8-147062,A, and JP,10-187618,A.
[0005]
[Problem(s) to be Solved by the Invention]However, when an inaccurate user starts a personal computer (personal computer) with a floppy disk in a Prior art, Although the application software on a personal computer cannot be started, since it is still possible, the copy and deletion of a file cannot be said to be that measures sufficient in the above-mentioned security countermeasures are taken.
[0006]Although security was considered by the whole system until now, it is thought by the fast improvement in the performance of a personal computer of late that the security countermeasures in each personal computer unit surface as an important problem from now on.
[0007]This invention is made in view of the problem in the illegal access prevention system of the above conventional computers, and is a thing.
The purpose is a powering-on stage of ** and is providing the illegal access prevention system and method of the computer which can prevent unjust access inside a personal computer.

[0008]
[Means for Solving the Problem]An illegal access prevention system of a computer by this invention is provided with the following.
It is an illegal access prevention system of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system, Said operating system is a Run-Time-Routine part of BIOS (Basic I/O System).
A Set-Up-Menu part of BIOS.
Have a password confirmation treating part and a password change treating part, and said password change treating part, Have a means for it to be controlled by said Set-Up-Menu part, and to set up a password beforehand, and said Run-Time-Routine part, A user starts with the directions after turning ON a power supply of a personal computer, and via a password confirmation treating part, By means to display a password input screen on said input/output device, and to demand password input from a user before starting said operating system, and the display of said password input screen. A means in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said

input/output device, When said password is inaccurate, a warning message is displayed on said input/output device, A means which will perform again a means urged to said password input if there is less display frequency of said warning message than prescribed frequency, and turns OFF a power supply of said computer when display frequency of said warning message is more than said prescribed frequency, A means by which there is nothing as if and said entered password starts said operating system to a right case.

[0009]An illegal access prevention system of a computer by this invention is provided with the following.
It is an illegal access prevention system of a computer which is provided with a display device and an input/output device containing a keyboard, and operates under control of an operating system, Said operating system is a Run-Time-Routine part of BIOS (Basic I/O System).
A Set-Up-Menu part of BIOS.
Have a password confirmation treating part and a password change treating part, and said password change treating part, Have a means for it to be controlled by said Set-Up-Menu part, and to set up a password beforehand, and said Set-Up-Menu part, A user starts with the directions after turning ON a power supply of a personal computer, and via a password confirmation treating part, By means to display a password input screen on said input/output device, and to demand password input from a user before starting said operating system, and the display of said password input screen. A means in comparison with a password beforehand set up by said password change treating part in a this entered password when a user entered a password from said input/output device, A means which turns OFF a power supply of said computer when said password is inaccurate, When there is nothing as if and collation of said password is able to be taken, it has a means to which a user is made to call said password change treating part with the directions from said input/output device, To a user said called password change treating part after this display with a means to display a message which makes it a purport whether to update a password or not on said input/output device from said input/output device. As a result of verifying a means to which the selection input of whether a password is updated or not is carried out, and the contents of this selection input, when an input of a purport that a password is updated is made, Write a password succeedingly entered from said input/output device in a management domain, and it sets up start an operating system in said Run-Time-Routine part, A means to start an operating system by said Run-Time-Routine part, A means by which said Set-Up-Menu part starts an operating system when an input of a purport that a password is updated is not made, as a result of there being nothing as if and verifying the contents of said selection input.

[0010]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described with reference to drawings.

[0011](A 1st embodiment) Drawing 1 is a block diagram showing the entire configuration of the illegal access prevention system of the computer concerning a 1st embodiment of this invention.
[0012]The illegal access prevention system of the computer concerning this embodiment is provided with the following.
The Run-Time-Routine part 1 of BIOS.
Password confirmation treating part 2.
The Set-Up-Menu part 3 of BIOS.
The password change treating part 4, and a display device, the input/output device 5 which consists of keyboards.

[0013]The password confirmation treating part 2 makes a password enter into a user in response to the demand from the Run-Time-Routine part 1 by him, when the power supply of a personal computer (personal computer) is turned ON by the user. As compared with the password succeedingly registered in the password entered by the keyboard of the input/output device 5 by the password change treating part 4 under Set-Up-Menu part 3 jurisdiction, if the password confirmation treating part 2 is a right password, it will start an operating system. A power supply is turned OFF after displaying the message of the purport that it is an inaccurate password on the display device of the input/output device 5, when the password entered [above-mentioned] was inaccurate, reinput is urged 3 times and an inaccurate password is still entered.
[0014]Drawing 2 is a flow chart which shows operation of the illegal access prevention system of the computer concerning a 1st embodiment of this invention.
[0015]Hereafter, referring to drawing 1, the flow chart shown in drawing 2 is used, and operation of the security system concerning this embodiment is explained.

[0016]First, in Step A, a user directs to start the Run-Time-Routine part 1, after turning ON the power supply of a personal computer.
[0017]The Run-Time-Routine part 1 starts with the directions from the above-mentioned user.
[0018]In Step B, with the directions from the Run-Time-Routine part 1 started [above-mentioned], before the password confirmation treating part 2 starts an operating system, it makes a password input screen display on the display device of the input/output device 5, and demands the input of a password from a user. Here, a user enters a password from the keyboard of the input/output device 5.
[0019]By the above-mentioned input request, if a user enters a password from the keyboard of the input/output device 5, at Step C the password confirmation treating part 2, When the above-mentioned password is inaccurate as compared with the password beforehand set up by the password change treating part 4, the password entered [above-mentioned], After the password confirmation treating part 2 displays a warning message on the display device of the input/output device 5 at Step D, The counter of the display frequency of a warning message is counted up, at Step F, if the display frequency of a warning message is to 2 times, it returns to Step B, and the input of a password is urged again. When the password which there is not as if and was entered [above-mentioned] is the 3rd inaccurate password entered from the keyboard of the input/output device 5, the password confirmation treating part 2 turns OFF the power supply of a personal computer.
[0020]In a right case, in Step C, the password entered [above-mentioned] starts an operating system.
[0021](A 2nd embodiment) The entire configuration of the illegal access prevention system of the computer concerning this example is the same as that of the illegal access prevention system of the computer concerning a 1st embodiment of this invention. However, the coordinated movements between the component differ from a 1st embodiment.
[0022]Drawing 3 is a flow chart which shows operation of the illegal access prevention system of the computer concerning a 2nd embodiment of this invention.
[0023]Hereafter, referring to drawing 1, the flow chart shown in drawing 3 is used, and operation of the security system concerning this embodiment is explained.
[0024]First, in Step A, a user directs to start the Set-Up-Menu part 3, after using the power supply ON of a personal computer.
[0025]In Step B1, with the directions from the Set-Up-Menu part 3 started [above-mentioned], before the password confirmation treating part 2 starts an operating system, it makes a password input screen display on the display device of the input/output device 5, and demands the input of a password from a user. Here, a user enters a password from the keyboard of the input/output device 5.
[0026]In Step C1, the password confirmation treating part 2 compares the password entered [above-mentioned] with the password beforehand set up by the password change treating part 4.
[0027]When collation of the above-mentioned password cannot be taken, the password confirmation treating part 2 turns OFF the power supply of a personal computer at Step D1 (when the password input by a user goes wrong).
[0028]When collation of the above-mentioned password is able to be taken, a user makes the password change treating part 4 call and perform by the keyboard of the input/output device 5 in Step E1 (when the password input by a user is successful).
[0029]Since the message "makes whether to update a password or not" a purport is displayed on the display device of the input/output device 5 by this, a user does the selection input of whether a password is updated or not from the keyboard of the input/output device 5. A user inputs "Yes" from the keyboard of the input/output device 5, when updating a password, and when not updating a password, he inputs "No" from the keyboard of the input/output device 5.
[0030]In step F1, the contents of the above-mentioned selection input are verified, and when the input of the purport that a password is updated is made, it moves to the following step G1 as it is. (When the input of the purport that a password is updated is not made, it moves to Step H1 which mentions a control flow later.) In Step G1, a user enters a password from the keyboard of the input/output device 5. The password entered [above-mentioned] is written in the area which the password change treating part 2 has managed.
[0031]In Step H2, the password confirmation treating part 2 sets up start an operating system in the Run-Time-Routine part 1, and starts the operating system by the Run-Time-Routine part 1.
[0032]In Step H1, the Set-Up-Menu part 3 starts an operating system.
[0033]Programs for making the above-mentioned processing perform to a processing unit, such as a program shown with the flow chart of drawing 2 and drawing 3, may be stored and distributed among the recording medium which CD-ROM etc. can computer read. And the computer which contains a microcomputer, a personal computer, and a general purpose computer in a category at least is good also as what reads the above-

mentioned program from the above-mentioned recording medium, and is performed.
[0034]
[Effect of the Invention]According to this invention explained above, unjust access to the computer which was not able to be prevented in the conventional operating system, It becomes possible to prevent in the powering-on stage of a personal computer, and it becomes possible to lose the copy of a file and worries about deletion according the operating system provided with abundant applications to an unauthorized use person, and to use it in comfort.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the entire configuration of the illegal access prevention system of the computer concerning a 1st embodiment of this invention.
[Drawing 2]It is a flow chart which shows operation of the illegal access prevention system of the computer concerning a 1st embodiment of this invention.
[Drawing 3]It is a flow chart which shows operation of the illegal access prevention system of the computer concerning a 2nd embodiment of this invention.
[Description of Notations]
1 Run-Time-Routine part
2 Password confirmation treating part
3 Set-Up-Menu part
4 Password change treating part
5 Input/output device

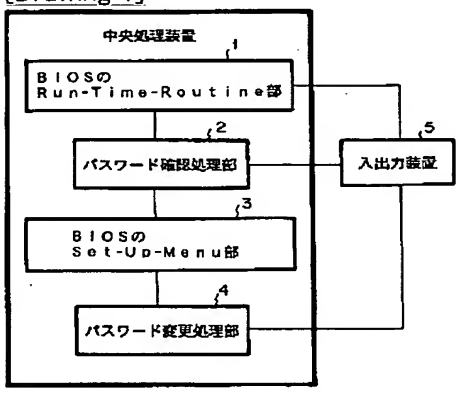
[Translation done.]

* NOTICES *

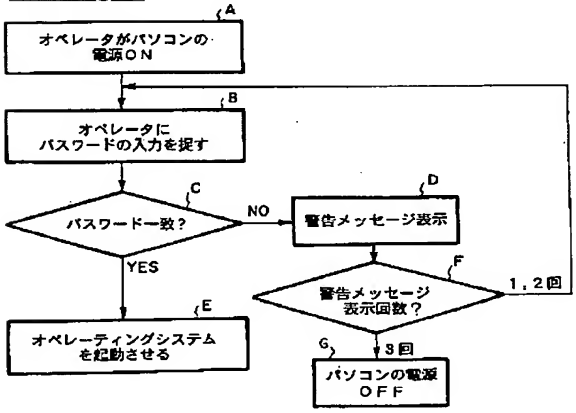
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

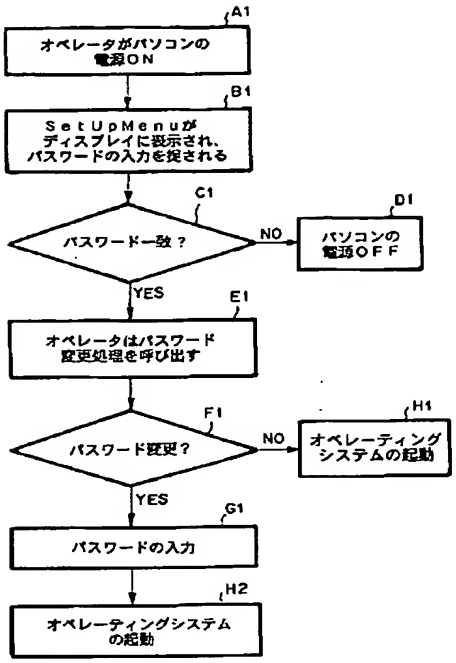
[Drawing 1]



[Drawing 2]



[Drawing 3]



[Translation done.]